SESAM
Försvarssektors användargrupp för Sofware Engineering

Generell riskkällechecklista

FMV dokumentbeteckning
14910:6057/2006

I-L Bratteby-Ribbing, FMV | Datum 2006-09-15 | Ver 1.3

Checklista allmänna riskkällor *(Generic Hazard Checklist)*

1 Syfte

Att i ett initialt skede av systemutvecklingen underlätta identifiering av möjliga riskkällor, genom att tillhandahålla en förteckning över allmänt kända riskkällor.

2 Skede

Främst vid PHL-analys samt PHA (se [6], [7]).

3 Begränsningar

En förteckning över allmänna riskkällor kan aldrig bli komplett. Av denna anledning har det kommit att utvecklas en mängd checklistor, som belyser skilda aspekter ur olika synvinklar. Några av dessa kan vara mer aktuella under tidig systemsäkerhetsanalys (t ex PHL-analys), andra är mer relevanta under en senare (t ex O&SHA), även om det givetvis är fördelaktigast att identifiera systemets riskkällor i ett initialt systemutvecklingsskede.
Denna sammanställning baseras på olika checklistor (med en del tillägg), vilket i princip ger högre täckning (om än till priset av viss överlappning)[1]. Samtidigt har vissa aspekter tonats ned i och med en fokusering mot riskkällor, vilka kan tänkas vara styrda, övervakade eller på annat sätt påverkbara av olika programvarusystem.

4 Riskkällor

4.1 Energiformer – Kraft

Mekanisk:
_ Potentiell
_ Kinetisk (Rörliga delar/föremål/projektiler)
_ Elastisk (Spänd fjäder)
_ Rotation (Propeller, Fläkt, Drivhjul)

Termisk:
_ Upphettade/nedfrysta föremål/vätskor/gaser (ånga)
_ Temperaturvariationer

Kärnenergi:
_ Restvärme
_ Radioaktivt avfall

Lagrad energi:
_ Tryckkärl/tryckkolv/gastub
_ Ackumulatorer/Kondensatorer
_ Spiralfjäderbelastade komponenter
_ Svänghjul
_ Upphängd/-hissad konstruktion/Reservoir/Cistern

Elektrisk[2]:
_ Felkoppling/Jordningsfel/Kortslutning
_ Överslag/Strömläckage/Urladdning/Strömbortfall
_ Överhettning/Antändning

Kemisk:
_ Bränsle
_ Ackumulatorer
_ Kemiskt inkompatibla föreningar/ämnen

Magnetisk:
_ Jordmagnetiska fältet

Strålning:
_ Röntgen/Radioaktiv (α/β/γ/Neutron)
_ Högeffektlaser/Infraröd/µ-våg/UV
_ Elektromagnetiska vågor

Massa[3]:
_ Fragment/Farkoster/Berg/Mark/Byggnader
_ Levande varelser (Människor, Djur)

Kraft (plötslig förändring av rörelsemängd/-hastighet/-riktning):
_ Acceleration (G-kraft, Jämvikts-/balansförlust)
_ Retardation (Inbromsning, Sammanstötning: Person-/Egendomsförlust/-skada [4], Flygande föremål, Jämnviktsförlust)
_ Gravitation (Fallande föremål)

---

[1] T ex kan uppdelningen i olika energiformer göras på flera sätt. Samma aspekt kan därför vara aktuell under flera rubriker.
[2] Typiska konsekvenser för denna riskkälla: Elchock/-stöt/-brännskada/brand.
[3] Även kroppar med låg masssa kan vid höga hastigheter ge katastrofala konsekvenser vid sammanstötning.
Ex: Fåglar som kolliderar med flygplan. Det frigolitfragment som 93-02-01 lossnade från Columbia-kapseln vid återinträde i atmosfären och skadade den värmeskyddande panelen i vänster vinge, vilken därefter smälte och kollapsade.

4.2 Materialegenskaper

Förgiftande/Kvävande/Förorenande/Frätande/Sjukdomsalstrande/Penetrerande:

_ Gas/Gift/Syra/Bakterie/Virus/Svamp/Skadedjur
_ Strålning (se 4.1)
_ Smuts/Förorening/Damm/Sand
_ Tung/Skarp/Vass/Skärande/Pressande del

i kombination med:

_ Materialutmattning/Korrosion/Nötning/Slitage/Kollaps
_ Hetta/Friktion/Sammanstötning/Hög-Låg fuktighets-grad
_ Silo-/Container-/Rörbristningar
_ Felkopplingar/Korskopplingar/Bakflöden

Lättantändlig:

_ Explosivämne: Bränsle/Bensin/Gas (Ånga)/Oxiderande ämne/Tändämne/Damm i kombination med
_ Utlösande faktor: Läckström, Gnista, Svetslåga, Hög(t) temperatur/tryck, Friktion, Vibration, Elektrostatisk urladdning

4.3 Omgivningsfaktorer

_ Driftsavbrott m a a: Gas/Vatten/El/Ventilation/Kylning/Uppvärmning/Smörjmedelsbrist.
_ Fukt/Ånga/(D)Imma/Underkylt regn/Is/Hagel/Snö/Vind/Storm
_ Extrema temperaturväxlingar/Hetta-Kyla-Frysning
_ Torrläggning/Översvämning/Överslag/Strömläckage
_ Hala ytor
_ Seismiska störningar/Åsknedslag
_ Störningar/Interferenser (EMI, RFI)
_ Vibrationer/Jordbävningar
_ Eld
_ Lufttryckfall/Syrebrist
_ Ljudtryck/Buller
_ Starkt ljus/Bländning
_ Lokalitet: Luftrum[5]/Berg/Hav/Mark/Bebyggelse/Skog/Öken/Arktisk zon

4.4 Användningsområde

Drift/användning

_ utanför avsedd användningsprofil
_ utanför avsedd omgivning[6].

4.5 Mänskliga faktorn

_ Felinstalleringar/felkalibreringar/felinställningar[7]/felbortkopplingar[8]
_ Operatörsfel[9]/Oavsiktlig aktivering/ Missuppfattning av information-status-position
_ Funktionsnedsättning/-bortfall/Handlingsförlamning/Utmattning/Trötthet/Otillgänglighet
_ Underhålls-/Översynsbrister

4.6 Systemfaser/-operationer/-mod[10]

_ Transport/Leverans
_ Parametersättning/Kalibrering
_ Installation
_ Leveranskontroll/Provning/Provtur
_ Simulering/Test/Utbildning[8]
_ Normal systemuppstart
_ Normaldrift
_ Driftsförändring/Modövergång/Upp-nedkoppling/Aktivering
_ Extrem driftmod/Degraderad driftmod
_ Nödstängning
_ Normal nedstängning
_ Underhåll/Felsökning

---

[4] Ex på en vanlig konsekvens: *Whiplash*-skada.
[5] Ex: Riskkällor vid hög höjd samt möjliga personskador: Kyla ⇒Förfrysning, Syrebrist ⇒Medvetslöshet.
[6] Ex: Flygning utanför tillåtna gränser/flygenvelopen.
[7] Ex: Felaktig installation av antikollisionssystemet TCAS. Se [9]:avsn 7 samt 12.5.2.
[8] Ex: Operatörernas bortkoppling/kortslutning av Tjernobyl-reaktorns nödkylnings- och skyddssystem. Se [9]: 12.5.1.
[9] Ex: Felaktigt val av kommando/operation, Reaktion för tidigt/sent, Inmatning i fel ordning, Aktivitet utförd för länge/kort.
[10] En komplettering behövs av det aktuella systemets faser/-moder. Ex:Taxning, Lättning, Flygning, Sättning, Parkering.

_ Nödstart

5 Referenser

[1] Uppdragsspecifkation SäkAnalysMetoder, FMVdokument 14910:88774/2005.
[2] Försvarsmaktens handbok för Systemsäkerhet, M7740-784851 H SystSäk, s 92 ff.
[3] Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar, M7762-000531 H ProgSäk
[4] Hazard Analysis Techniques for System Safety, C.A. Ericsson, ISBN 0-471-72019-4, s 62 ff + App C.
[5] System Safety Analysis Handbook, www.system-safety.org/ProductsSale.php, s 3-209 ff.
[6] PHL-analys, Faktablad för Preliminär riskkällelista, FMVdokument 14910:2662/2006.
[7] PHA, Faktablad för Preliminär riskkälleanalys, FMVdokument 14910:2795/2006.
[8] System Safety Hazard Checklist, System Safety Scrapbook Sheet 86-1, www.svedrup.com/safety/scrapbook.shtml.
[9] Programvarusäkerhet –en introduktion, FMVdokument KC Ledstöd 14910:38346/02.

6 Dokumenthistorik

Version	Datum	Beskrivning
1.0	06-03-01	Faktablad enl [1]: uppgift 4. För komplettering under SESAM:s påföljande analysmöten.
1.1	06-05-03	Smärre kompletteringar under 4.2 efter möte 06-04-07.
1.2	06-08-18	Smärre kompletteringar under 4.2-4.3.
1.4	06-09-15	Smärre kompletteringar under 4.2, 4.6 baserat på [8], [9].